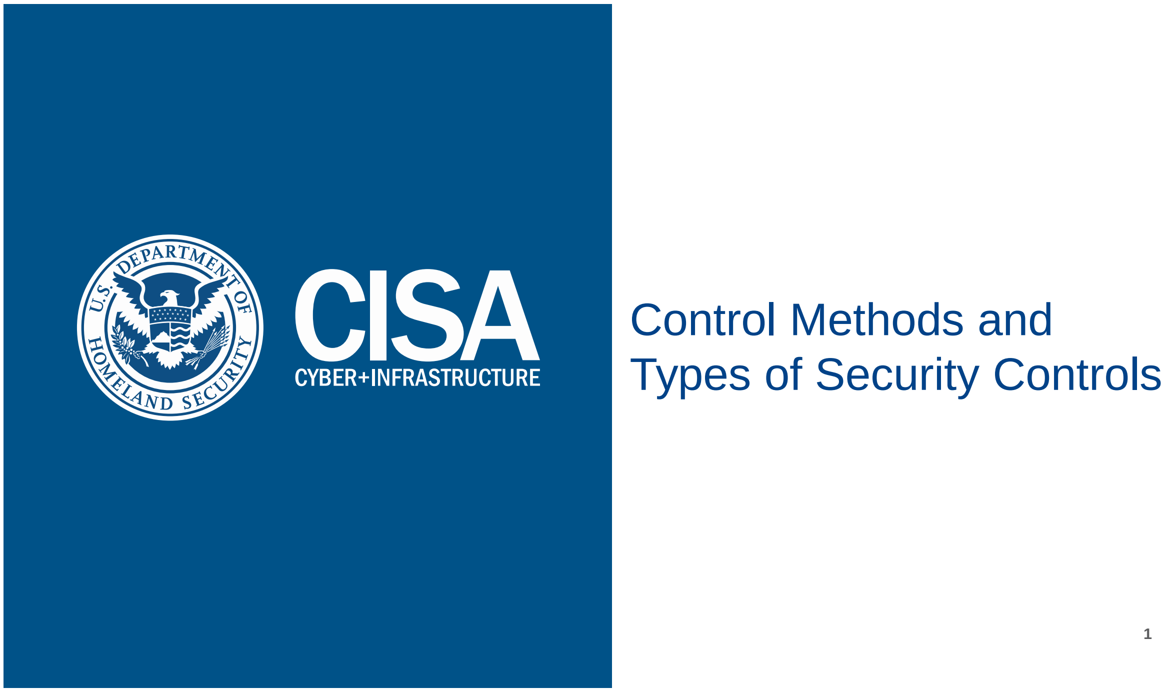
Control Methods and Types of Security Controls

Table of Contents

Control Methods and Types of Security Controls

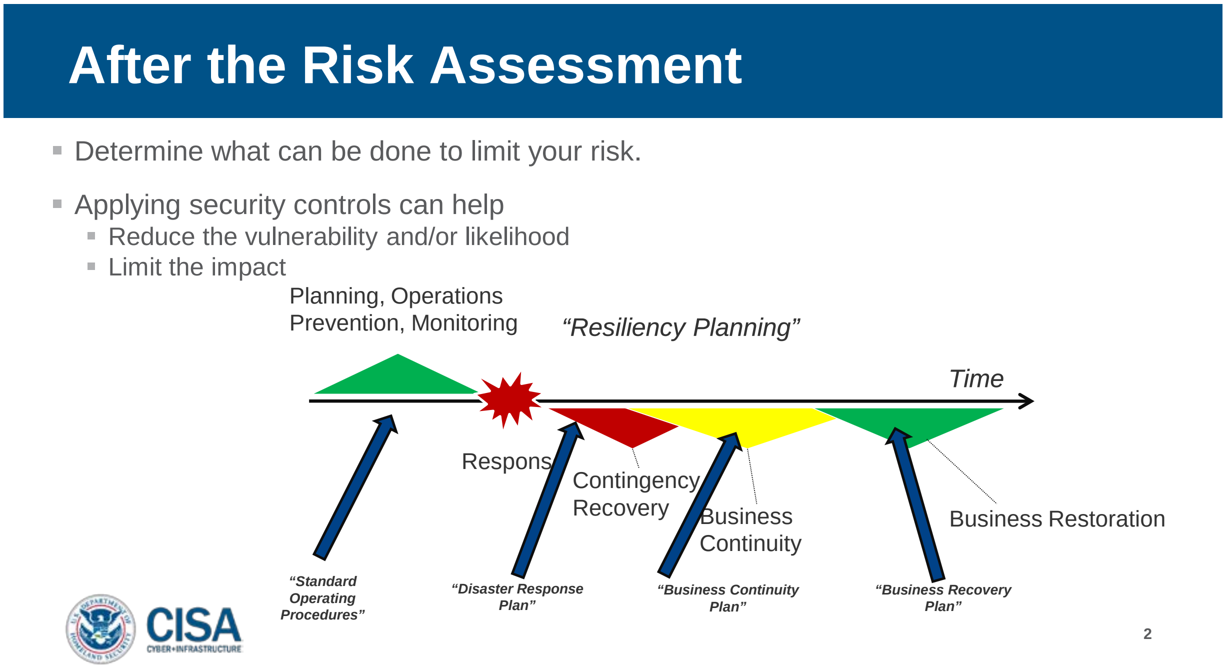

U.S. DEPARTMENT OF HOMELAND SECURITY
CISA
CYBER+INFRASTRUCTURE

Control Methods and
Types of Security Controls

1

**001 Instructor: Today I'm going to talk about control methods and types of security controls that you can implement on your system.

After the Risk Assessment

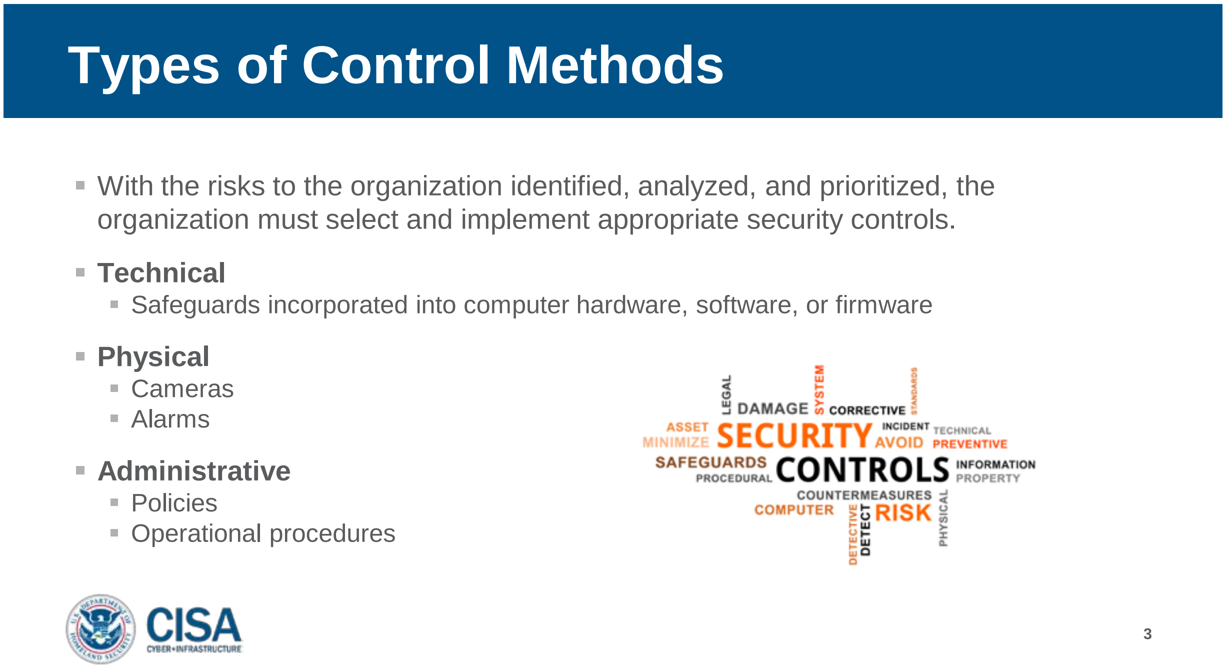


After the Risk Assessment

- Determine what can be done to limit your risk.
- Applying security controls can help
  - Reduce the vulnerability and/or likelihood
  - Limit the impact

**002 Now remember that risk happens over a timeline. So we may have normal operations, and at some point an incident will take place, and you're going to respond to that, and then you may have to take subsequent actions to get your organization back up and running. But for today, what I want to talk about is what we're going to do to limit the up-front actual event from actually taking place. Some of it may help you with the impact down the road, but for the most part what we're talking about here are controls that keep the risks from actually coming to fruition.

Types of Control Methods



Types of Control Methods

- With the risks to the organization identified, analyzed, and prioritized, the organization must select and implement appropriate security controls.
- **Technical**
  - Safeguards incorporated into computer hardware, software, or firmware
- **Physical**
  - Cameras
  - Alarms
- **Administrative**
  - Policies
  - Operational procedures

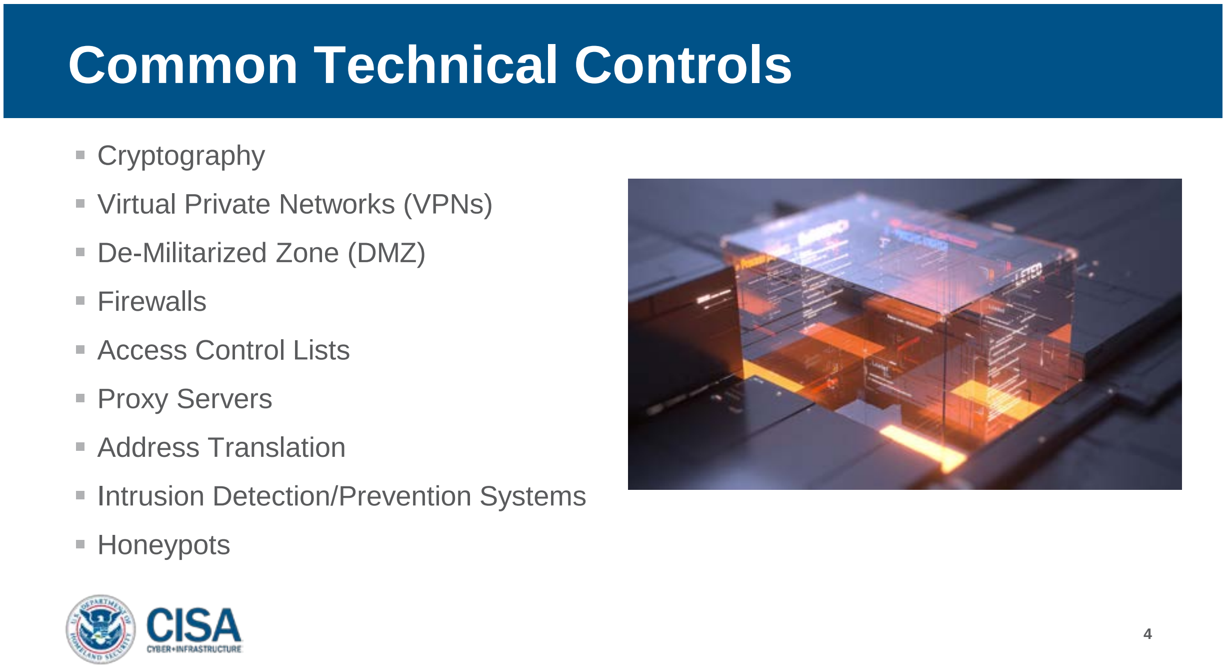
LEGAL
DAMAGE
SYSTEM
CORRECTIVE
STANDARDS
ASSET
MINIMIZE
SECURITY
INCIDENT
AVOID
TECHNICAL
PREVENTIVE
SAFEGUARDS
PROCEDURAL
CONTROLS
INFORMATION
PROPERTY
COUNTERMEASURES
COMPUTER
DETECTIVE
DETECT
RISK
LEGAL
PHYSICAL
CISA
CYBER+INFRASTRUCTURE
3

**003 So there are types of control methods that you can put in place. There are three primary types, actually: technical, physical, and administrative. An example of a technical control would be like a firewall, for example-- some piece of hardware or software or something that you put in your system that can actually prevent threat actors from coming in and taking adverse action on your system.

There's also physical controls. These are things that you can put up in your actual facility, if you will, so that you can prevent people from moving to where they shouldn't be, or to keep threat actors out. Examples of things that you can use here for monitoring would be cameras, alarms, fences, door locks, things of that nature.

You may also have something like administrative control methods. These are written policies or procedures that people inside the organization and outside the organization may have to follow so that way they can do business with you, or work for you, for that matter.

Common Technical Controls



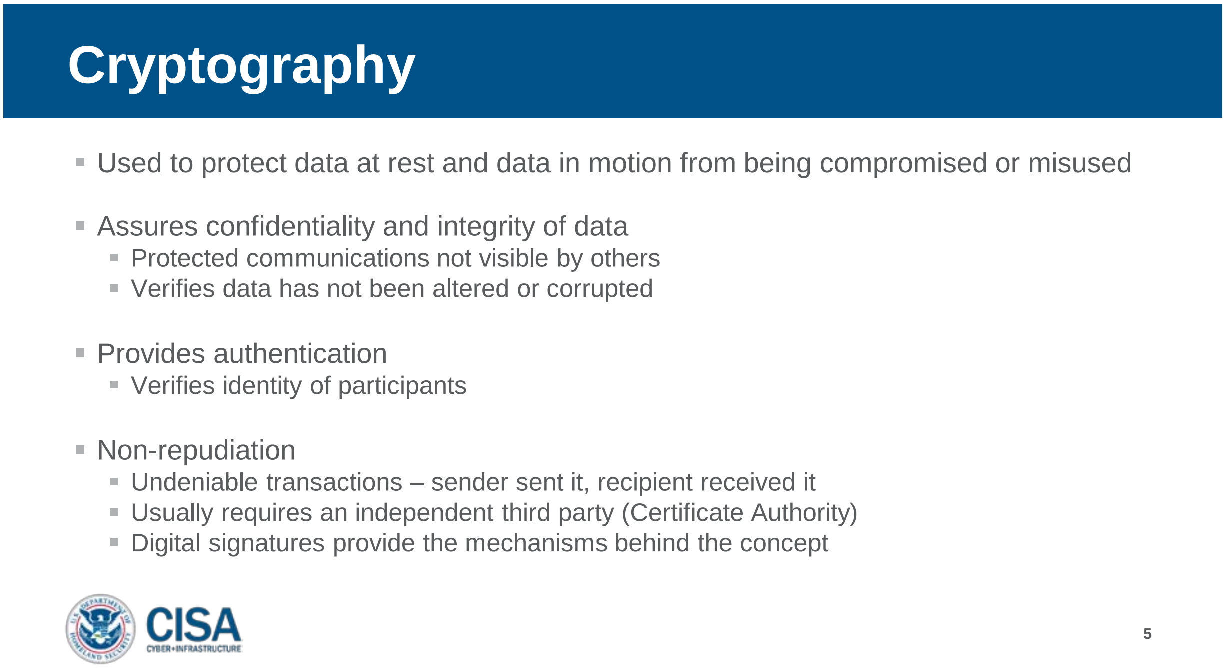
Common Technical Controls

- Cryptography
- Virtual Private Networks (VPNs)
- De-Militarized Zone (DMZ)
- Firewalls
- Access Control Lists
- Proxy Servers
- Address Translation
- Intrusion Detection/Prevention Systems
- Honeypots

4

**004 So let's talk a little bit about common technical controls. As you can see from this slide, there are a lot of them to cover. And by the way, this list in and of itself is not even exhaustive. This is a real high-level treatment of these just to give you a little bit of background so you can go do your own research and figure out what's best for your organization.

Cryptography



Cryptography

- Used to protect data at rest and data in motion from being compromised or misused
- Assures confidentiality and integrity of data
  - Protected communications not visible by others
  - Verifies data has not been altered or corrupted
- Provides authentication
  - Verifies identity of participants
- Non-repudiation
  - Undeniable transactions – sender sent it, recipient received it
  - Usually requires an independent third party (Certificate Authority)
  - Digital signatures provide the mechanisms behind the concept

**005 Let's start with cryptography, and I'm sure many of you have heard about this, and I know it makes your head hurt, and you start thinking about big mathematical problems. But really what it comes down to is you're protecting your data in terms of confidentiality, integrity, and its nonrepudiation.

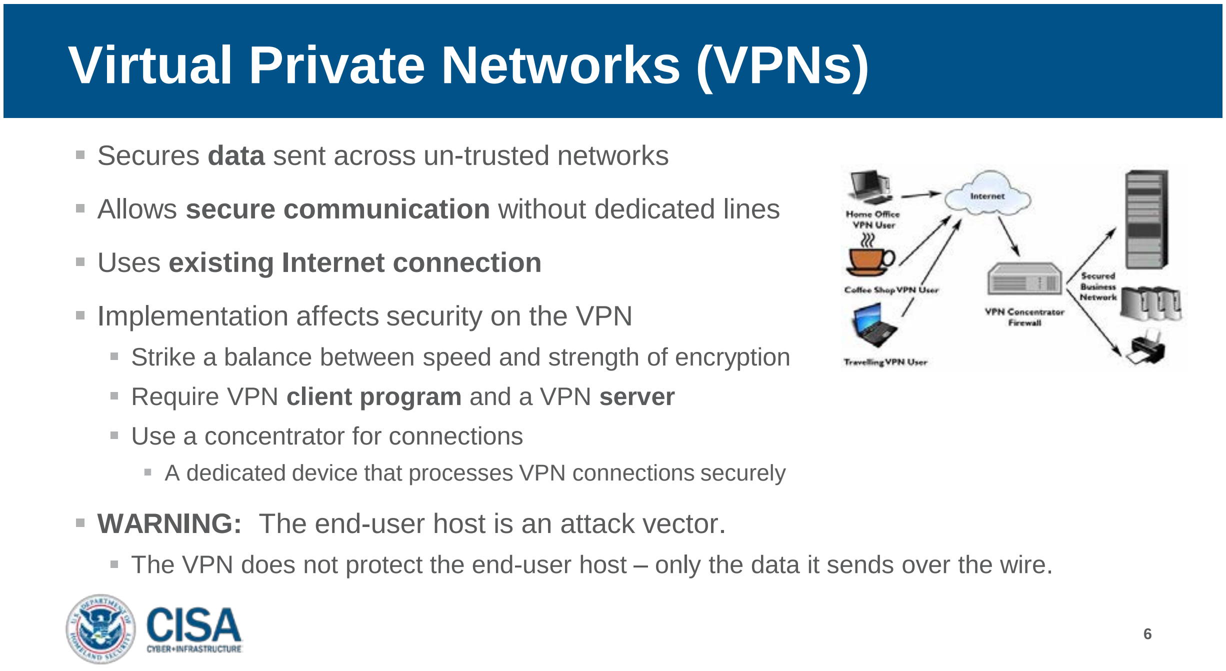
So let's talk about this at each step. What you really want to do is you want to make sure that this information does not go broadly to the public because it has some sort of confidentiality element to it. So cryptography, if we actually scramble up a message and make sure that people can't understand what the information is or that the data is exactly, we've actually ensured some element of confidentiality there.

There is also this element of having people actually change the data. Maybe they do it with malicious intent. What we want to do is we want to protect the integrity of that data. So we can use cryptography to do things like hashing, so that way we can actually condense a message, and if that condensed message changes in any way, shape or form, we know that the integrity has been violated.

We can also use cryptography to understand if there's been some sort of person who has received the information and we need to know if in fact they did receive it, and they get some sort of certificate authority to help them with that so that we understand that the third-party is in receipt and they actually are the people that they say that are that received it. We call this nonrepudiation.

We also may need to use cryptography when you log into your computer every day. This is when you do some sort of authentication. It makes sure that you're the right person to enter into a system, or have access to a certain level or degree.

Virtual Private Networks (VPNs)



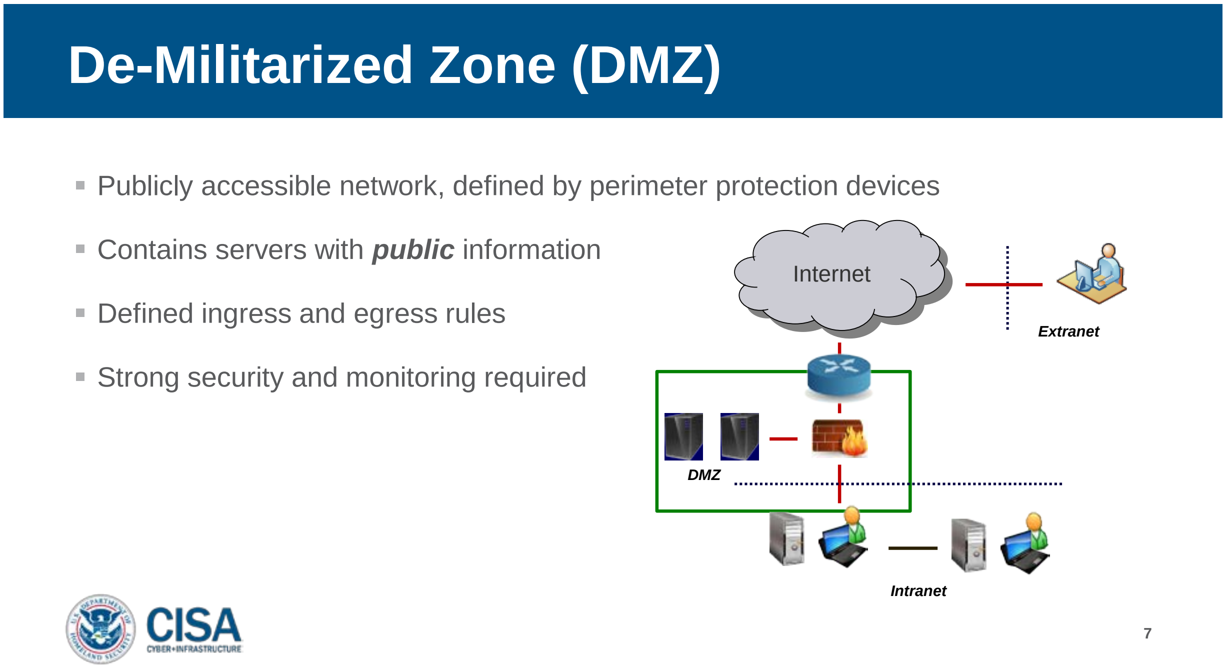
Virtual Private Networks (VPNs)

- Secures **data** sent across un-trusted networks
- Allows **secure communication** without dedicated lines
- Uses **existing Internet connection**
- Implementation affects security on the VPN
  - Strike a balance between speed and strength of encryption
  - Require VPN **client program** and a VPN **server**
  - Use a concentrator for connections
    - A dedicated device that processes VPN connections securely
- **WARNING:** The end-user host is an attack vector.
  - The VPN does not protect the end-user host – only the data it sends over the wire.

**006 Now, we may actually want to move this information around. We may actually want to operate over a network, and we may or may not be in our organization resident on a secure connection with our network. We can use virtual private networks to help us with this. Think of this as nothing more than a lead pipe that fluid will go through and nothing can penetrate that pipe to get to that fluid. That fluid is your data and information, and a VPN provides that kind of protection around it, and they do this mathematically with encryption. It's a secure communication, like a pipeline, if you will. What you have is information that will go from where you're operating; it will go typically to some kind of concentrator, especially if there's multiple streams of information that's coming in from multiple users, and then it will be able to go to your server.

Now you got to remember here that there is the chance that the end-user who actually has the information could be doing bad things. The VPN just protects the information as it's in motion. It's not necessarily protecting the endpoints. Keep that in mind.

De-Militarized Zone (DMZ)



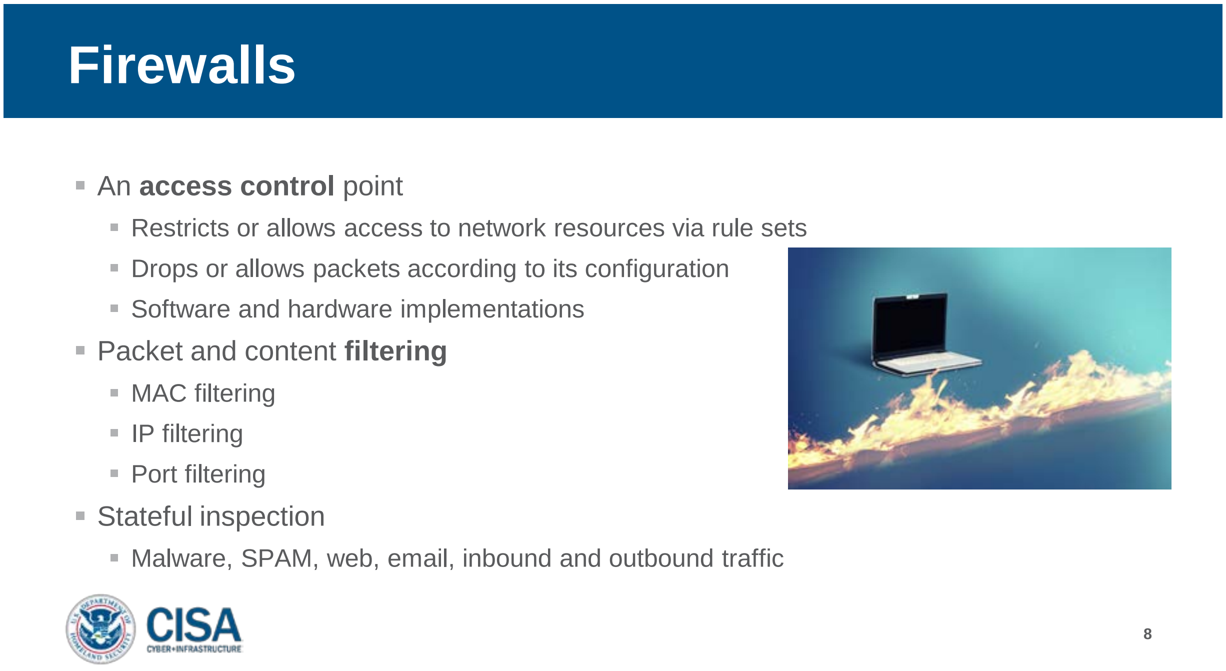
De-Militarized Zone (DMZ)

- Publicly accessible network, defined by perimeter protection devices
- Contains servers with ***public*** information
- Defined ingress and egress rules
- Strong security and monitoring required

**007 You may also want to establish what's called a demilitarized zone. I like to think of this with the analogy of having a castle. So you may think of your castle being your system in and of itself, your intranet, and what I really want to do is I want to communicate with the outside world-- the people, the things that are outside the gates of my castle. And I may have firewalls, I may have some kind of protection zone that keeps people from actually getting into the castle. Sometimes I may even want to let them know within that firewall so that way they can look at maybe a website or something I've set up for them. We can set this up and call it a demilitarized zone. Think of it as the courtyard that's around the castle, if you will, and the castle itself still has walls to get through and gates to get through to actually get to the high-value assets.

Now, there could be rules or guards that are actually enforcing these rules at each step of the process as they get from different points in this demilitarized zone. You're going to want to think about who's going to have access to each of these elements, and you're going to have strong security in between each of these elements to ensure the security of the assets within.

Firewalls



Firewalls

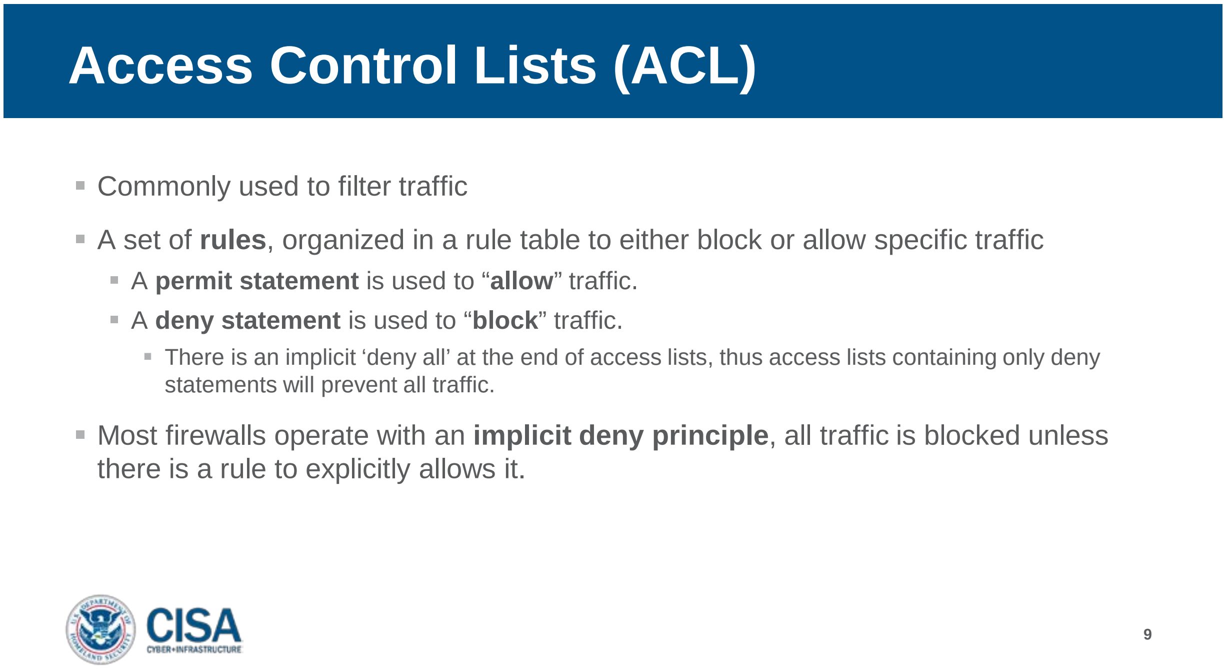
- An **access control** point
  - Restricts or allows access to network resources via rule sets
  - Drops or allows packets according to its configuration
  - Software and hardware implementations
- Packet and content **filtering**
  - MAC filtering
  - IP filtering
  - Port filtering
- Stateful inspection
  - Malware, SPAM, web, email, inbound and outbound traffic

8

**008 I just mentioned firewalls, and in that analogy I just gave, this would be the walls of your castle, basically, with specific access control points. You're allowing information into your enterprise and you're letting it come out of your enterprise. The firewall can actually be somewhat smart about this, and actually monitor the individual information packets that are coming to your organization, and as it does, it can decide what are the good ones and what are the bad ones. There are different ways we can do this, and we call this filtering. There could be MAC filtering, IP filtering, port filtering. It all depends on what point you want to look at that data entering the system and how you want to look at it.

Let's give an example. For example, in a stateful inspection, what I'm actually going to do is I'm looking for packets that are coming into the system and actually also looking at where the traffic has come from and where it's going to. This could be important information in terms of discerning what's important and maybe what is a bad actor.

Access Control Lists (ACL)



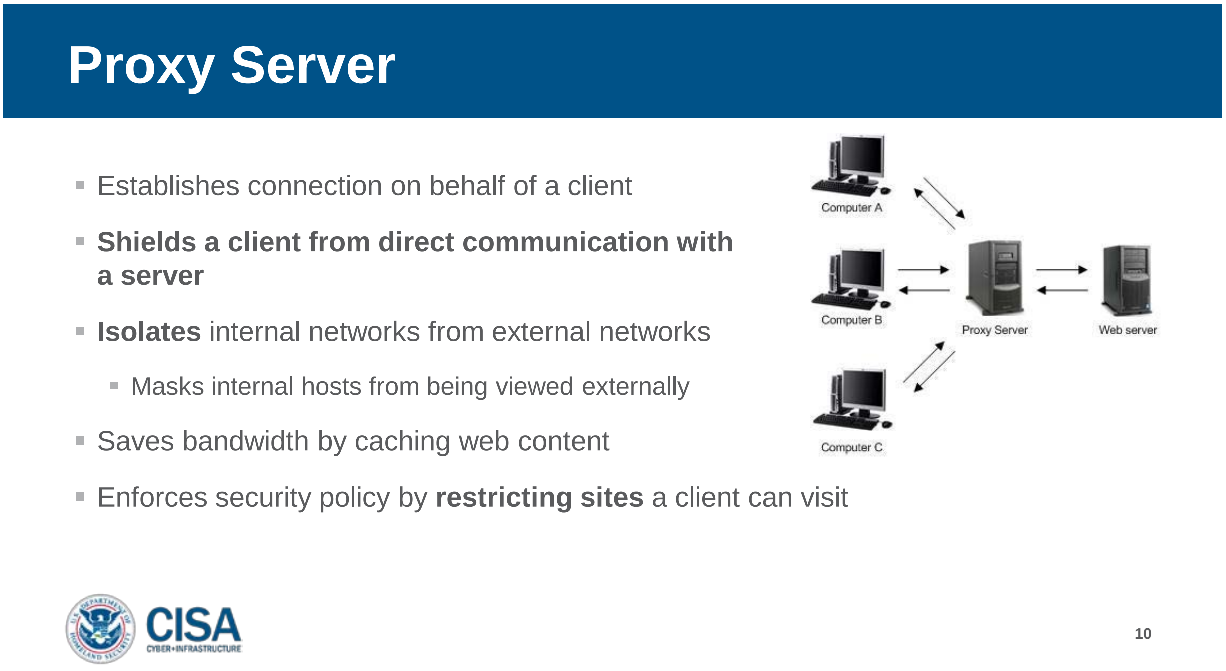
Access Control Lists (ACL)

- Commonly used to filter traffic
- A set of **rules**, organized in a rule table to either block or allow specific traffic
  - A **permit statement** is used to "**allow**" traffic.
  - A **deny statement** is used to "**block**" traffic.
    - There is an implicit 'deny all' at the end of access lists, thus access lists containing only deny statements will prevent all traffic.
- Most firewalls operate with an **implicit deny principle**, all traffic is blocked unless there is a rule to explicitly allows it.

9

**009 I could also use access control lists. These are commonly used to filter traffic as well, similar to a firewall, but basically what they are is they're a set of rules that I have to allow traffic in or block it if I find out that it's not good. Let's also talk about the idea that these firewalls operate off an implicit deny principle. That means that all the traffic is blocked unless there's a rule that allows it to actually come into the system.

Proxy Server

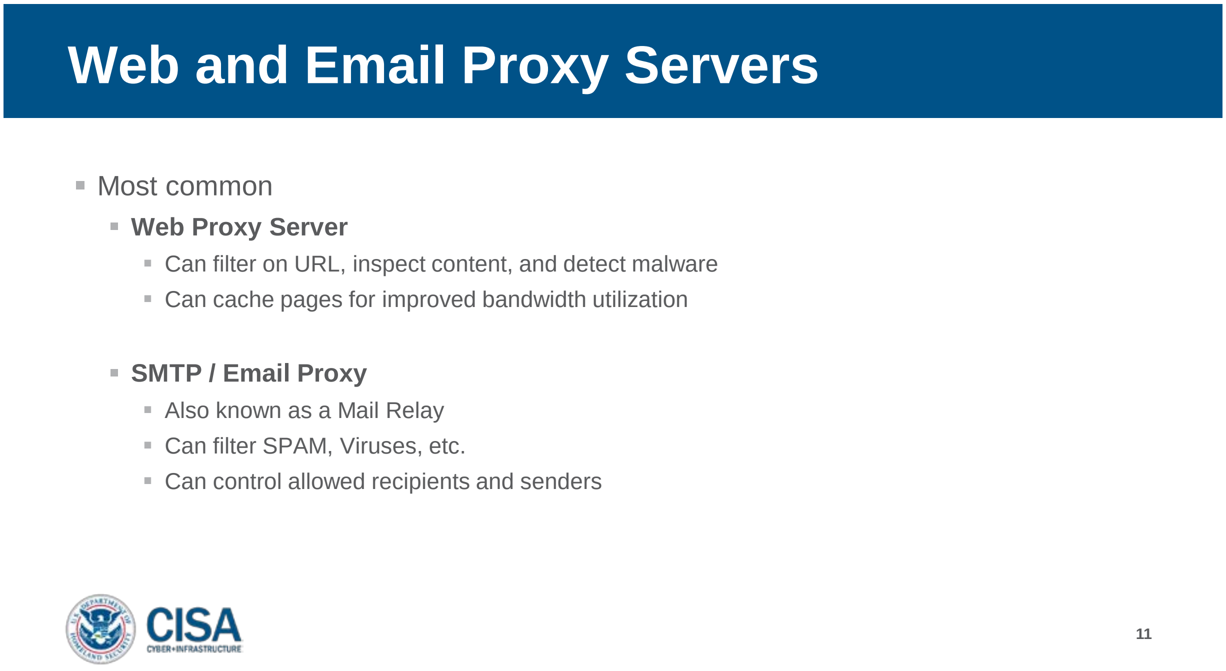


Proxy Server

- Establishes connection on behalf of a client
- **Shields a client from direct communication with a server**
- **Isolates** internal networks from external networks
  - Masks internal hosts from being viewed externally
- Saves bandwidth by caching web content
- Enforces security policy by **restricting sites** a client can visit

**010 I also may want to operate with a little bit of insulation around who is actually coming onto my servers. Now, I may also want to shield my client from direct communication with that server. If that's the case, I can set up a proxy. Think of this as a stand-between between my actual server itself and those clients that are operating it to get information from it. It isolates my internal networks from my external ones, and it actually masks what those internal ones may be, so that way I can't come in and just look at what's inside your house, if you will. It's almost like a window, if you will, but the window has shades for certain clients. Some can see more than others.

Web and Email Proxy Servers



Web and Email Proxy Servers

- Most common
  - **Web Proxy Server**
    - Can filter on URL, inspect content, and detect malware
    - Can cache pages for improved bandwidth utilization
  - **SMTP / Email Proxy**
    - Also known as a Mail Relay
    - Can filter SPAM, Viruses, etc.
    - Can control allowed recipients and senders

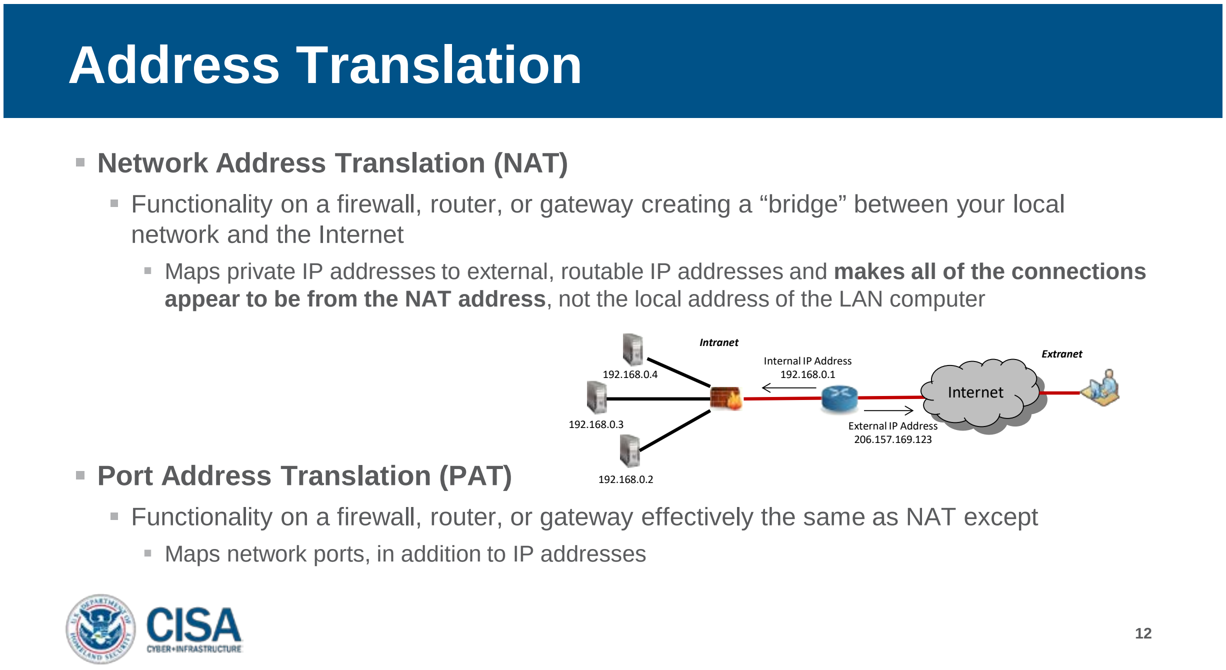
CISA
CYBER+INFRASTRUCTURE

11

**011 On these proxy servers, there are different types. Some common ones that you may come in contact with are web proxy servers, where I can actually filter upon different URLs and I can look at different content that may be coming and going, and I can even cache pages or store them, if you will, for future use. That way it doesn't have to reload the page time and again.

There's also an email proxy server. You may be very familiar with this if you've heard of SMTP, and the idea that your email is actually sitting out there somewhere as you look at it, and it gets downloaded to your inbox every day. That's typically email sitting on a proxy server. It can also be helpful because on this server we could be filtering for spam or viruses, or messages that we know are malicious to the organization.

Address Translation



Address Translation

- Network Address Translation (NAT)
  - Functionality on a firewall, router, or gateway creating a “bridge” between your local network and the Internet
    - Maps private IP addresses to external, routable IP addresses and **makes all of the connections appear to be from the NAT address**, not the local address of the LAN computer

- Port Address Translation (PAT)
  - Functionality on a firewall, router, or gateway effectively the same as NAT except
    - Maps network ports, in addition to IP addresses

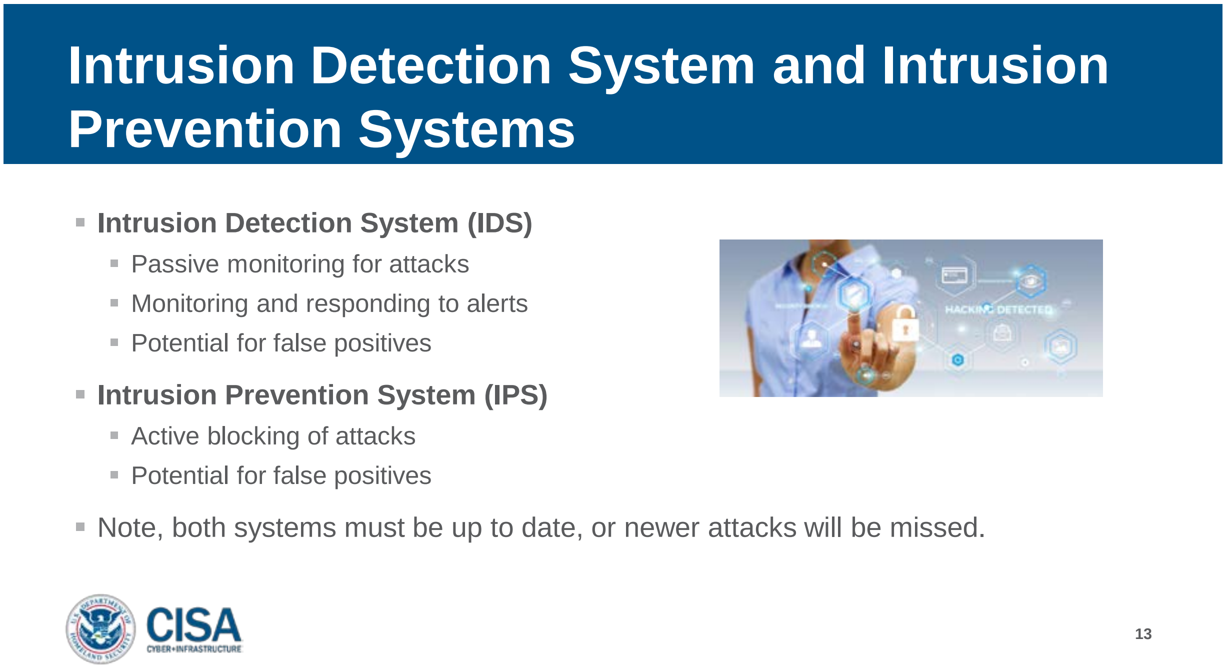
CISA
CYBER+INFRASTRUCTURE

12

**012 We can also think about this in terms of masking what we're actually doing in a sense with respect to working on this network. We can use what's called a network address translation, a NAT. What we're doing here is we're creating a bridge between our local network and the actual internet, and we want to mask what we're actually doing in terms of connections. That NAT is going to give just a general address so that way people who are external to the internet won't know what the address is in the actual network that they're working with.

Another form of address translation is port address translation, and this is very similar to a NAT, but what we're doing is we're also masking the network ports that can be actually accessed, as well as IP addresses.

Intrusion Detection System and Intrusion Prevention Systems



Intrusion Detection System and Intrusion Prevention Systems

- **Intrusion Detection System (IDS)**
  - Passive monitoring for attacks
  - Monitoring and responding to alerts
  - Potential for false positives
- **Intrusion Prevention System (IPS)**
  - Active blocking of attacks
  - Potential for false positives
- Note, both systems must be up to date, or newer attacks will be missed.

HACKING DETECTED

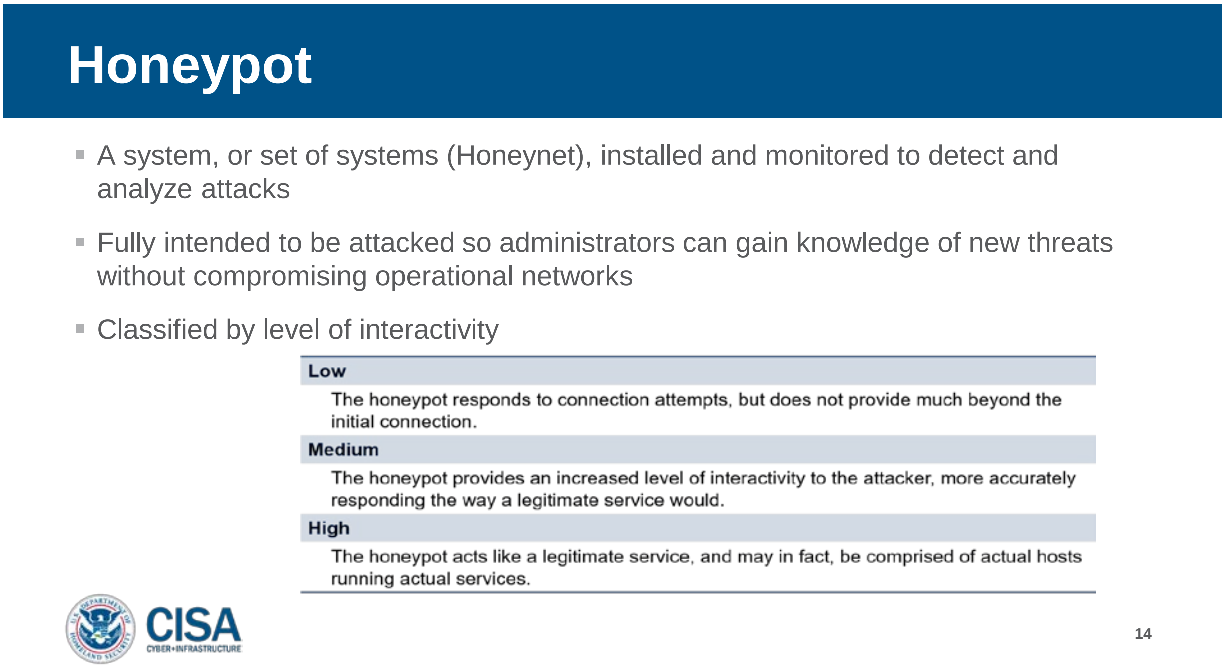
13

**013 Now, we could also have intrusion detection systems and intrusion prevention systems. What we're doing here is we're really trying to understand if there's any malicious actors that have actually gotten into the system. It may be just a matter of having a loud dog in your house that barks if you have bad guys get in. That would be an example of an intrusion detection system. The dog's not going to do anything. Maybe it's sitting in its crate and it's just barking really loud. It provides alerts. Now the problem here is that you could have false-positives. Suppose it's your in-laws who come over for a visit and they're more than welcome, but the dog's still going to bark. So you got to be mindful of that, because it could have a lot of false-positives.

You could also think about it as the dog now being free from the crate and actually taking action to scare the intruders away. This could be thought of as an intrusion prevention system, where I'm actually actively blocking these attacks coming in the system, especially once I've detected them.

So note, if you're going to do this and use an IDS and IPS, make sure that they're up to date. They have to be aware of signatures of what's trying to get in the system and what's getting out, and this only comes with understanding and knowing what the newer attacks look like.

Honeypot



Honeypot

- A system, or set of systems (Honeynet), installed and monitored to detect and analyze attacks
- Fully intended to be attacked so administrators can gain knowledge of new threats without compromising operational networks
- Classified by level of interactivity

Low

The honeypot responds to connection attempts, but does not provide much beyond the initial connection.

Medium

The honeypot provides an increased level of interactivity to the attacker, more accurately responding the way a legitimate service would.

High

The honeypot acts like a legitimate service, and may in fact, be comprised of actual hosts running actual services.

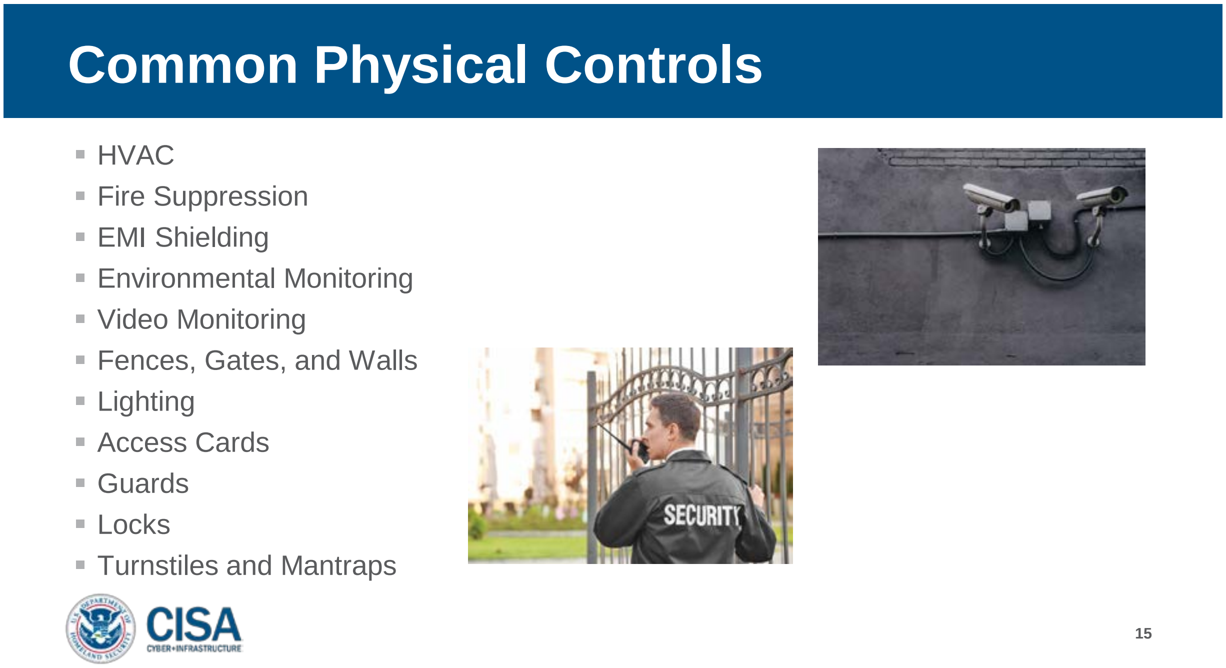
CISA CYBER+INFRASTRUCTURE

14

**014 Another instrument we could use is a honeypot. This is nothing more than a system that can actually be used to understand what kind of threats you may be having coming into your system. Think of it as a computer system that people can access, but it really leads to nowhere. It's almost like a maze that you put in front of your front door that people could get lost in-- the attackers could get lost in, that is. And there's different levels of interactivity that you could have here. You could have a honeypot that is a low interactivity level, which means that basically an attacker is only going to be able to make a connection, and it doesn't really get much beyond that.

It graduates from there, because I could have an attacker that will actually get in the system, and maybe it can actually get some kind of response going, and actually similar to what a service would provide. I can even up that a little bit more and have a higher level of fidelity, and it can actually have a host where I'm actually running critical services-- actual services, excuse me-- that the attacker may at least be baited into thinking that this is a real valid server and something that they could get some critical information off of.

Common Physical Controls



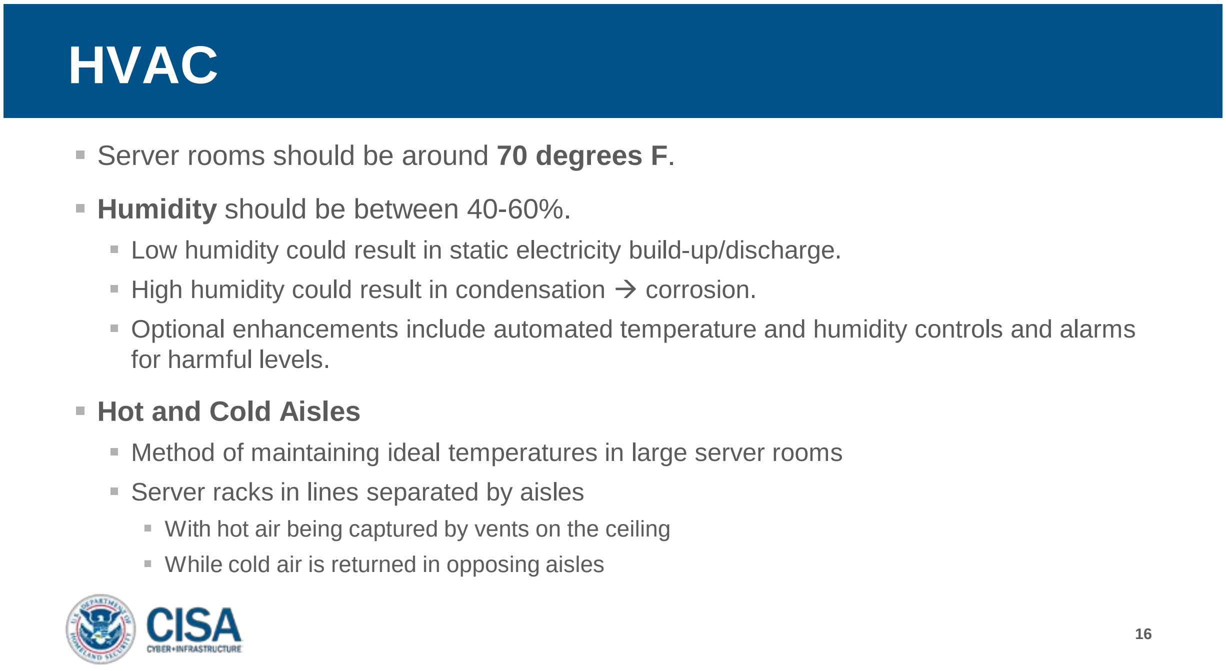
Common Physical Controls

- HVAC
- Fire Suppression
- EMI Shielding
- Environmental Monitoring
- Video Monitoring
- Fences, Gates, and Walls
- Lighting
- Access Cards
- Guards
- Locks
- Turnstiles and Mantraps

SECURITY
CISA
CYBER+INFRASTRUCTURE
15

**015 So now that we've talked about technical controls, let's talk about some physical controls as well. As you can see, there are a lot to be discussed here, and we're going to stick to a high level with them.

HVAC



HVAC

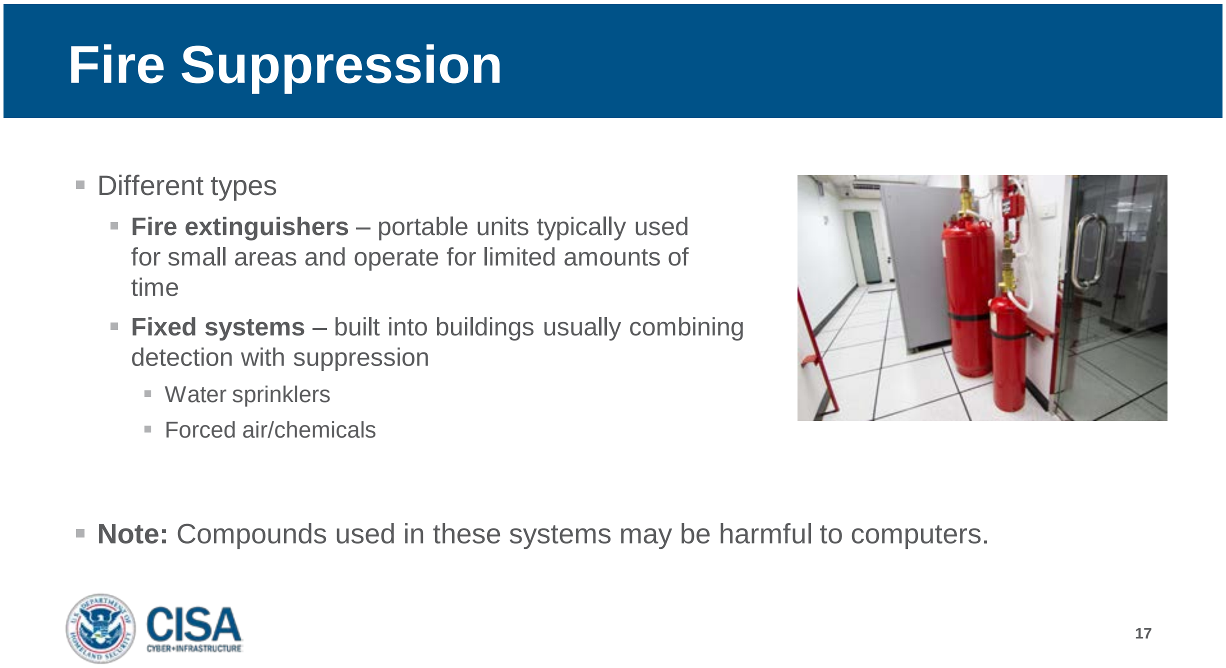
- Server rooms should be around **70 degrees F**.
- **Humidity** should be between 40-60%.
  - Low humidity could result in static electricity build-up/discharge.
  - High humidity could result in condensation → corrosion.
  - Optional enhancements include automated temperature and humidity controls and alarms for harmful levels.
- **Hot and Cold Aisles**
  - Method of maintaining ideal temperatures in large server rooms
  - Server racks in lines separated by aisles
    - With hot air being captured by vents on the ceiling
    - While cold air is returned in opposing aisles

16

**016 So first let's talk about HVAC. This is going to be things like your ventilation within your building. You're going to think about your server room specifically. Now these servers can be kind of finicky in terms of the environment that they're in. Ideally you want to be around 70 degrees or so, which is actually a little cooler than you might believe, especially if you have to spend a good day with them. You also have to think about how humid it is in the environment it's in. Typically it's between 40 and 60 percent, is the ideal. Either way, if you get low humidity, what you could have is a static electricity buildup, and this could discharge and damage your equipment. If you have high humidity, you could have condensation, which could lead to corrosion in your equipment, maybe even some shorts. So you got to be careful and monitor this humidity and control it closely.

You also want to think about how you set up your servers. You may want to set it up such that you have hot aisles and cold aisles, and what you want to do is strike an ideal temperature balance within these large rooms. You separate them by aisles so that way the air can circulate around.

Fire Suppression



Fire Suppression

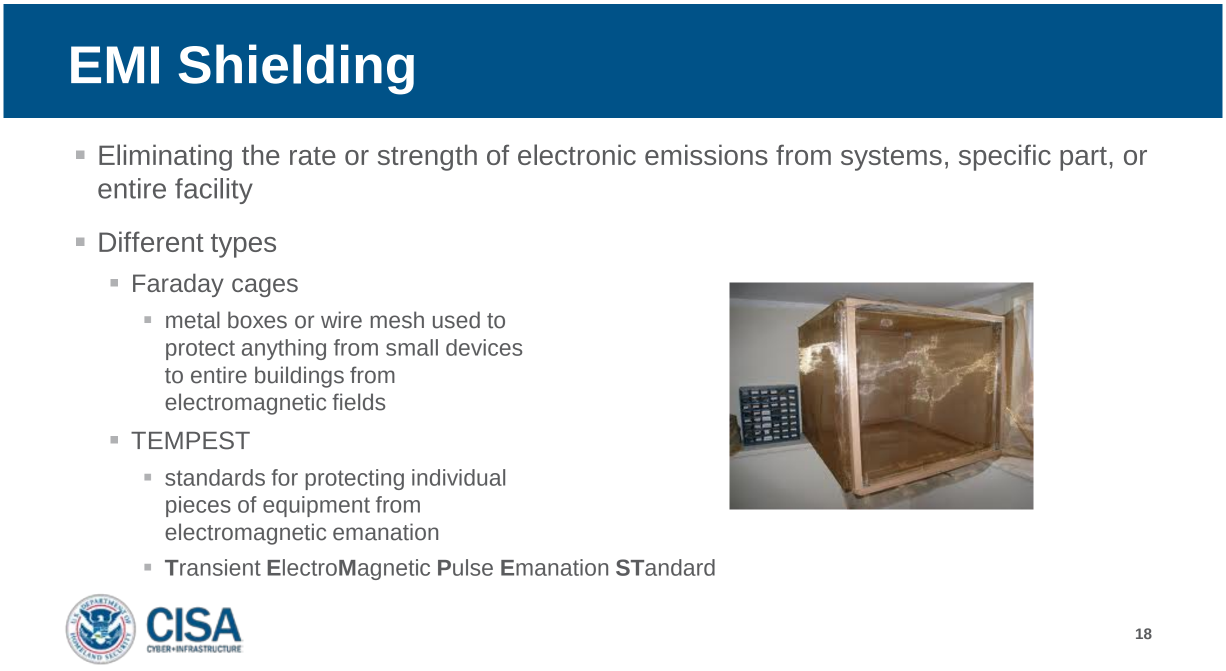
- Different types
  - **Fire extinguishers** – portable units typically used for small areas and operate for limited amounts of time
  - **Fixed systems** – built into buildings usually combining detection with suppression
    - Water sprinklers
    - Forced air/chemicals

- **Note:** Compounds used in these systems may be harmful to computers.

17

**017 You may also want to think about fire suppression. We all fear fire, no matter what, and it's not uncommon to have them in server rooms, especially where you have a lot of electrical equipment. But once again, this technical equipment can be very finicky in terms of what you use in terms of agents for extinguishing these fires. So if you want to think about using fire extinguishers, you may want to, for example, use CO2 extinguishers for electrical fires. Water sprinklers, eh, yeah, they may be good, especially for Class A type fires that are made of paper products, but water sprinklers clearly are going to damage the electrical equipment. In that case, forced air or chemicals may be better. Warning: Sometimes even some chemicals can be bad for equipment. For example, purple potassium powder, PKP, can be found in some fire extinguishers. It's extremely corrosive to electrical equipment. So you need to be mindful of what compounds you're using for what equipment you're trying to protect.

EMI Shielding



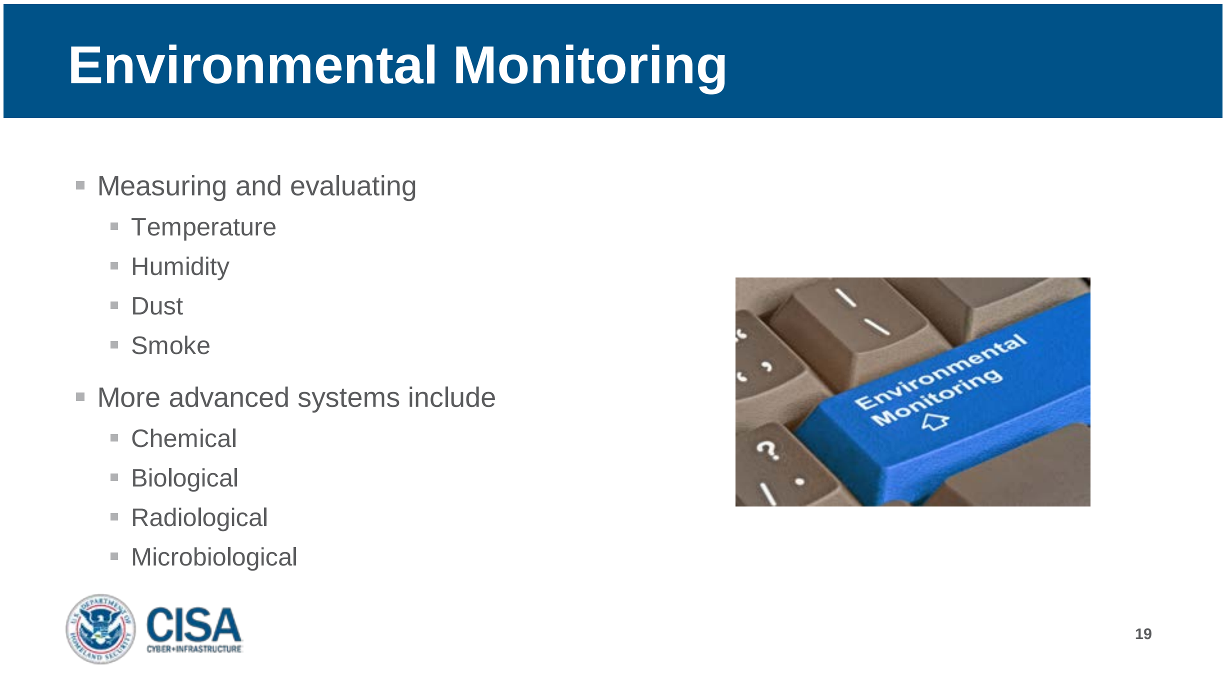
EMI Shielding

- Eliminating the rate or strength of electronic emissions from systems, specific part, or entire facility
- Different types
  - Faraday cages
    - metal boxes or wire mesh used to protect anything from small devices to entire buildings from electromagnetic fields
  - TEMPEST
    - standards for protecting individual pieces of equipment from electromagnetic emanation
    - **T**ransient **E**lectro**M**agnetic **P**ulse **E**manation **ST**andard

18

**018 Now, we could also have electromagnetic interference shielding. Basically, if someone were to walk into one of our computer server rooms with a high-power radio, that radio could generate some sort of inductive reaction within the equipment and it would actually damage the equipment or maybe interrupt it. So what we'll do is we could set up things called Faraday cages, which is basically like a big metal wire mesh box that you could put around your equipment, and it would interrupt or interfere with that signal actually getting to the equipment. Now, there are some programs that you can research on this. One is called TEMPEST, which stands for Transient Electromagnetic Pulse Elimination Standard. They provide a good number of things that you can do to insulate your equipment in a reasonable way.

Environmental Monitoring



Environmental Monitoring

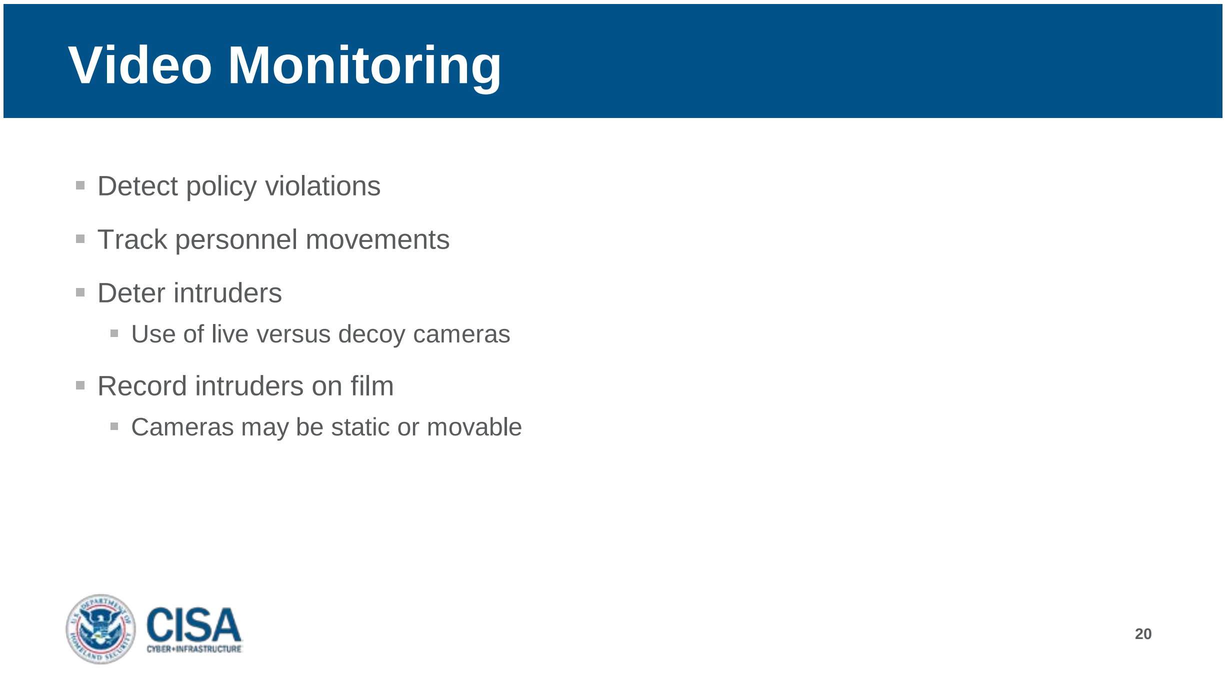
- Measuring and evaluating
  - Temperature
  - Humidity
  - Dust
  - Smoke
- More advanced systems include
  - Chemical
  - Biological
  - Radiological
  - Microbiological

Environmental
Monitoring

**019 We also want to think about how we're going to monitor our environment. I've already talked about humidity and temperature, but you may want to think about some other things. How much dust do you have in your environment? Is there any smoke? You may look for incipient conditions that precede a fire and actually have alarms set up to warn you before you even get to that point.

You could also have systems that think about detecting things like different chemicals that may be in a space, maybe even biological, or maybe you have radiation sources that could be a concern.

Video Monitoring



Video Monitoring

- Detect policy violations
- Track personnel movements
- Deter intruders
  - Use of live versus decoy cameras
- Record intruders on film
  - Cameras may be static or movable

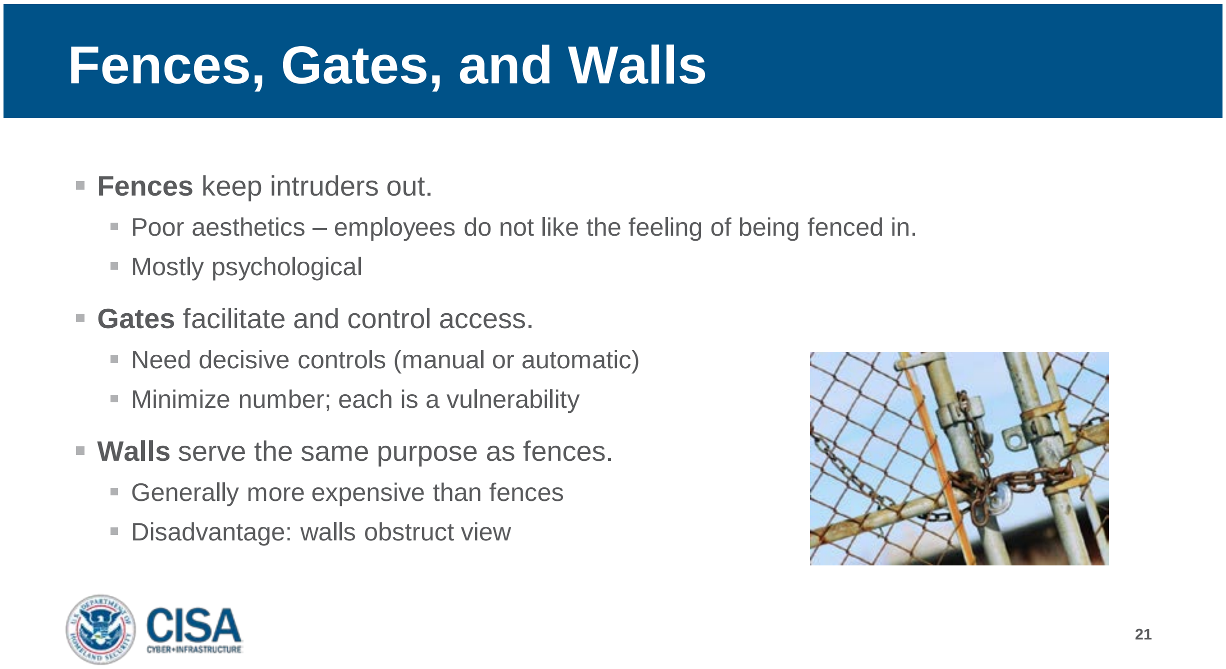
CISA
CYBER+INFRASTRUCTURE
20

**020 We talked a little bit about video monitoring. This is how you're going to monitor areas that you want to detect where you may have some sort of violation, whether it's people in the wrong space or people doing the wrong thing. If you want to track personal movements, video monitoring is likely one of your answers. Now you got to be mindful of this one because it could get quite expensive, not only in terms of equipment, but now I have to have somebody actually monitor the equipment. I actually have to have somebody physically watching the monitors to make sure that the policies are being followed.

Now truly I could be recording and I could use it as a forensic type piece of equipment, but if that's the case, then you're really losing a fundamental capability that you're trying to seek with that video monitoring. You may just have some decoy cameras set up, because if you could think about it, you can actually just be deterring intruders who know better, if they see the camera, not to do things that are bad.

If you are recording, you could also have different types of cameras that are static versus movable. In other words, a static camera is going to be looking down one hallway in one direction, and maybe that's all the camera does at all times. Or you could have a camera that trains so that you get a full sweep of a certain area.

Fences, Gates, and Walls



Fences, Gates, and Walls

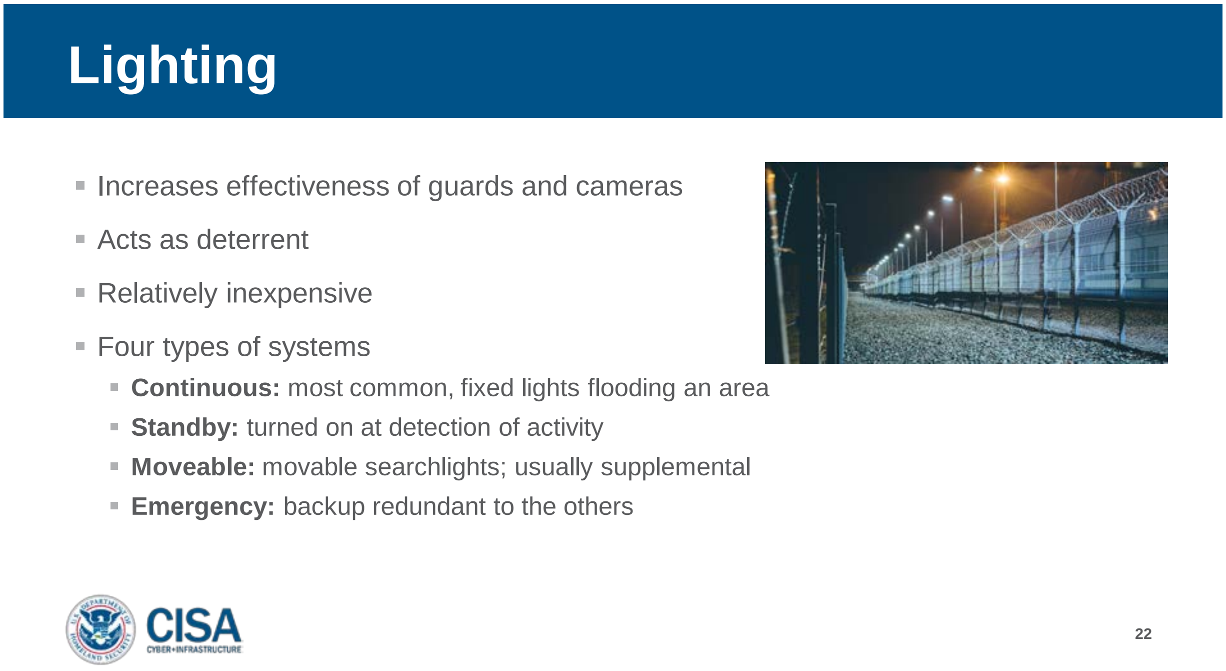
- **Fences** keep intruders out.
  - Poor aesthetics – employees do not like the feeling of being fenced in.
  - Mostly psychological
- **Gates** facilitate and control access.
  - Need decisive controls (manual or automatic)
  - Minimize number; each is a vulnerability
- **Walls** serve the same purpose as fences.
  - Generally more expensive than fences
  - Disadvantage: walls obstruct view

**021 You may also have fences, gates, and walls that you set up around your organization, and it really depends not only aesthetically on what you want to do, but it also depends on what kind of security you want to have. Fences clearly are going to keep intruders out, but if you have a standard cyclone fence, it really kind of looks industrial to say the least. So aesthetics may not be there. And also you've seen people who have the ability to quickly climb those fences. Some people may say that this is mostly psychological. It can be a deterrent all the same, so don't discount it.

Gates-- now this is how you're going to actually control access through those fences or walls. Now, you're going to want to have some kind of control mechanism on these gates. They may be manual; they may be automatic. Manual, for example, would be maybe you have an actual physical lock and key on it. Automatic, maybe you have some kind of infrared detection that actually opens the gate when it senses somebody coming. Now, you're going to have to have them have a key of some sort too. Maybe they have some kind of RFID or a badge or something like that that they swipe that they get in. Maybe you have a gate guard that's actually watching too. Either way, you want to be mindful of how many gates you have around your facility and what kind of access they're allowing at any given point in a day.

You may also put up walls, and this serves the same purpose as fences, but generally they're a little bit more expensive. The other thing you got to think about is people behind the wall cannot see what's going on beyond the wall, unless you have cameras obviously set up. So this could be a disadvantage.

Lighting



Lighting

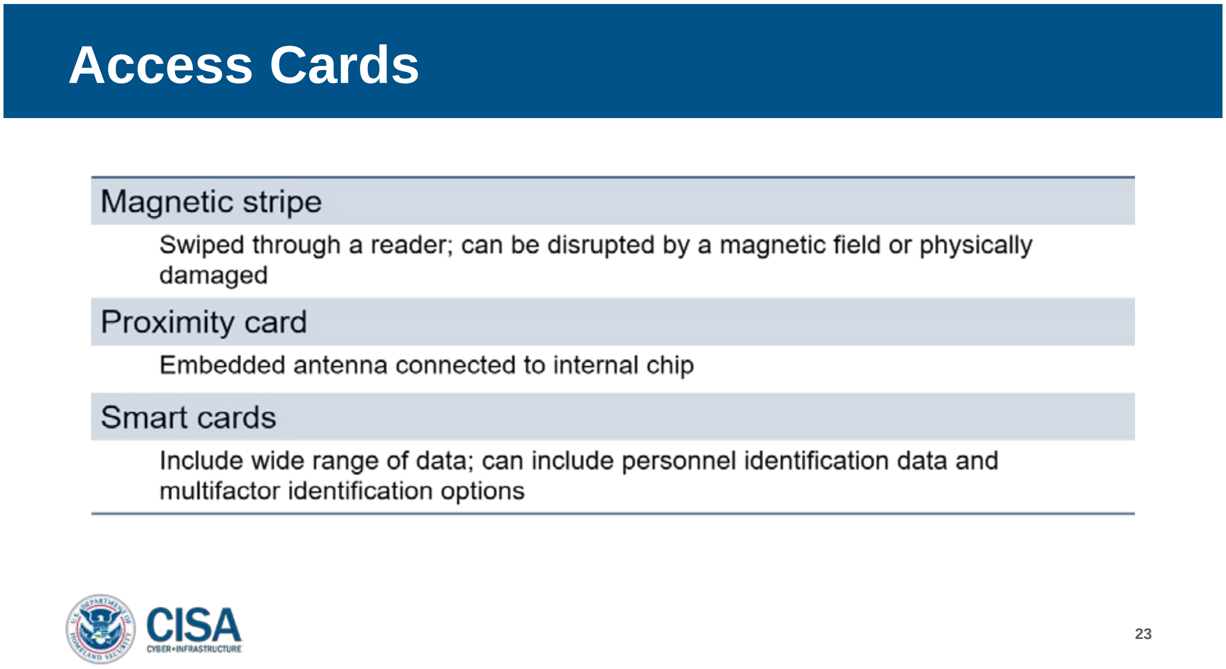
- Increases effectiveness of guards and cameras
- Acts as deterrent
- Relatively inexpensive
- Four types of systems
  - **Continuous:** most common, fixed lights flooding an area
  - **Standby:** turned on at detection of activity
  - **Moveable:** movable searchlights; usually supplemental
  - **Emergency:** backup redundant to the others

22

**022 Lighting is also very important, and relatively speaking, it's inexpensive compared to other deterrents that I've provided you here. If you think about it, it's a deterrent right off the bat because if people don't want to be seen doing surreptitious things, then lighting is good for you. There are different types of systems you can set up too. You can have it just have one light that continuously on, and this is typically most common, especially for flooding broad areas with light. You can have lights on standby; so in other words, they're looking for motion detection or maybe a heat signature to turn on. Lights can be movable. This is the classic movie that you watch where you have prison guards and they're actually scanning a certain area with a movable light. That can be done automatically or it can be done manually.

You could also have emergency lighting. Now this is important not just in terms of intrusion, but let's suppose that you have a site outage, and it's important to get around that site safely. Emergency lighting would be a consideration here.

Access Cards



Access Cards

Magnetic stripe

Swiped through a reader; can be disrupted by a magnetic field or physically damaged

Proximity card

Embedded antenna connected to internal chip

Smart cards

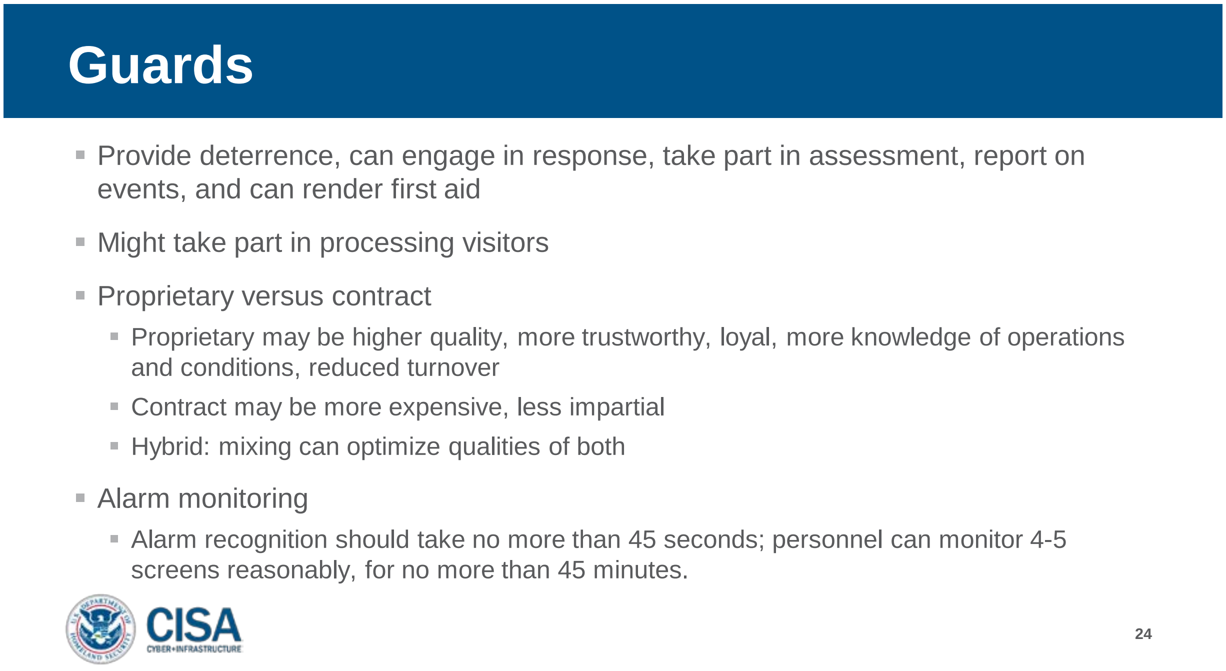
Include wide range of data; can include personnel identification data and multifactor identification options

23

**023 So let's go back to that discussion about gates again, because what you really want to do is you want to control access to and from. We used to have keys, and we still do largely, but it may be more helpful to have access cards, and there are different types you may want to consider. There are magnetic stripe cards, and this would look like your general credit card. It can be swiped through a reader, but you got to be mindful of the fact that they can be somewhat fragile. They can easily be disrupted with magnetic fields, and they're pretty easily damaged too.

You can also use proximity cards. It's basically a plastic card that has an antenna embedded in it with a chip, and you can swipe it in front of a reader and it will actually allow access if it identifies correctly with that card. There are also smart cards, and they can contain a whole wide range of data on them. This includes personal identification type data. So these are classic type badges-- or classic type cards that can be used as badges in a facility too, and really are especially helpful if you want to have multifactor authentication available to you.

Guards



Guards

- Provide deterrence, can engage in response, take part in assessment, report on events, and can render first aid
- Might take part in processing visitors
- Proprietary versus contract
  - Proprietary may be higher quality, more trustworthy, loyal, more knowledge of operations and conditions, reduced turnover
  - Contract may be more expensive, less impartial
  - Hybrid: mixing can optimize qualities of both
- Alarm monitoring
  - Alarm recognition should take no more than 45 seconds; personnel can monitor 4-5 screens reasonably, for no more than 45 minutes.

CISA CYBER+INFRASTRUCTURE

24

**024 Aha. Now we've talked about this. You could actually have guards that you pay to actually work for you to make sure that people are following rules, and they're especially helpful if you want to provide deterrent, because if someone sees a guard, clearly they're not going to want to be around if they're thinking to do adverse things. Guards are helpful too because they can actively engage in response, not just for security instances too. Suppose you have somebody that gets injured at a site. They can actually be a first responder force. They can actually take part in assessments too and be active participants. They can actually report on events, more so than just a camera just capturing what's going on. They can provide more context for an event too. They can also take part in controlling the flow of physical traffic to and from and in and out of a facility.

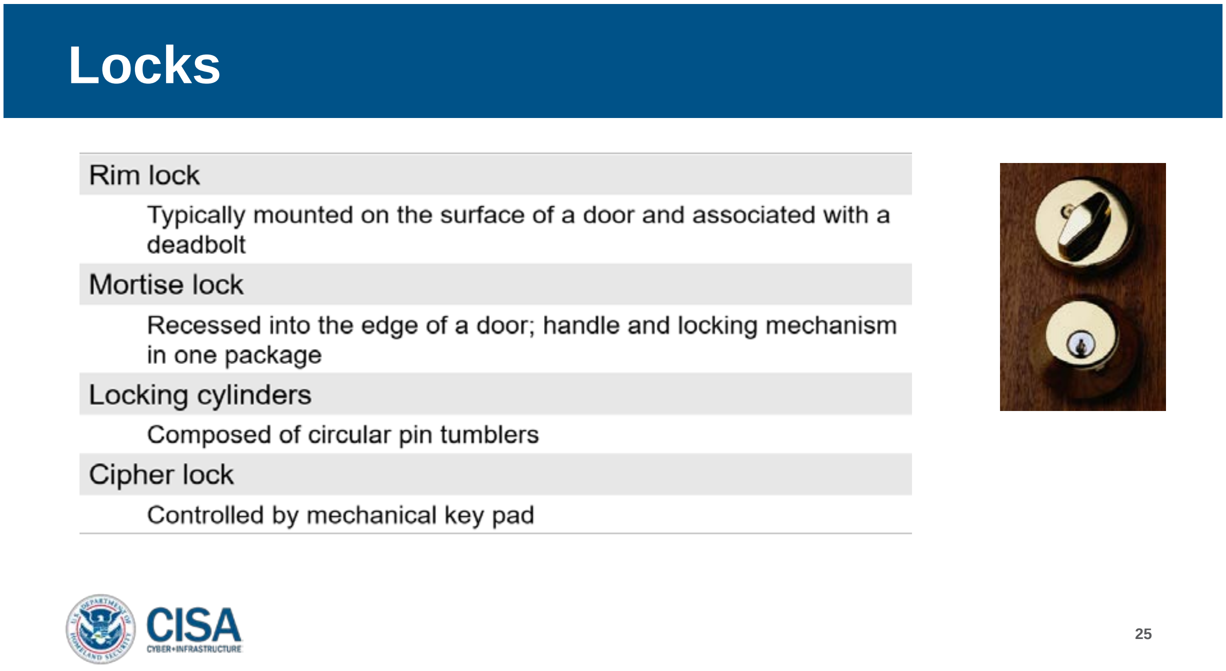
Now, you want to think about what kind of guard force you want to have. You may actually hire your own personal guard force and pay for them out of your own budget, or you may actually go to a third-party vendor and actually not have them in the employee base. So you may think of people that you actually hire within your organization being a little bit more trustworthy and loyal, at least to the extent that they understand the culture of your organization a little better. Now by the way, that might change over time. You may have hired this third-party guard force and over time, sure, they will get to know your organization better. But you would like to think that your employees would have a little bit more knowledge of your operations and conditions, especially at first. You may also-- hopefully you're paying your employees well-- have a little bit less in terms of turnover.

Now, if you think about it, contracts can be expensive, so you got to be careful there as well. You got to make sure that the balance of having a contracted guard force is right for you in terms of what you're willing to pay. Go back to that risk assessment, make sure that your analysis, your cost-benefit analysis, tells you that it's something that you really want to have.

You can also have a mix, where you have an employed guard force and a guard force that you've hired to be, say, part-time, to support and supplement.

You can also set up alarms, and these can be set up for any amount of time for any area, that kind of a thing. So what you want to do is you can have delays on the alarm. Suppose you only expect a pass-through point, and maybe a person is supposed to be through that pass-through point for no more than a certain amount of time. You can set that alarm to go off if that person is there any longer than they have to be. A classic example of this would be a door alarm. How many times have you gone through a door and after so many seconds, especially in an airport, the alarm starts going off. That's a classic example of alarm monitoring. Guards can really be helpful with this because sometimes even people who are there who are actively engaged may not really know what to do and may not be engaged enough to feel that they have responsibility to respond to that alarming condition.

Locks



Locks

Rim lock

Typically mounted on the surface of a door and associated with a deadbolt

Mortise lock

Recessed into the edge of a door; handle and locking mechanism in one package

Locking cylinders

Composed of circular pin tumblers

Cipher lock

Controlled by mechanical key pad

CISA

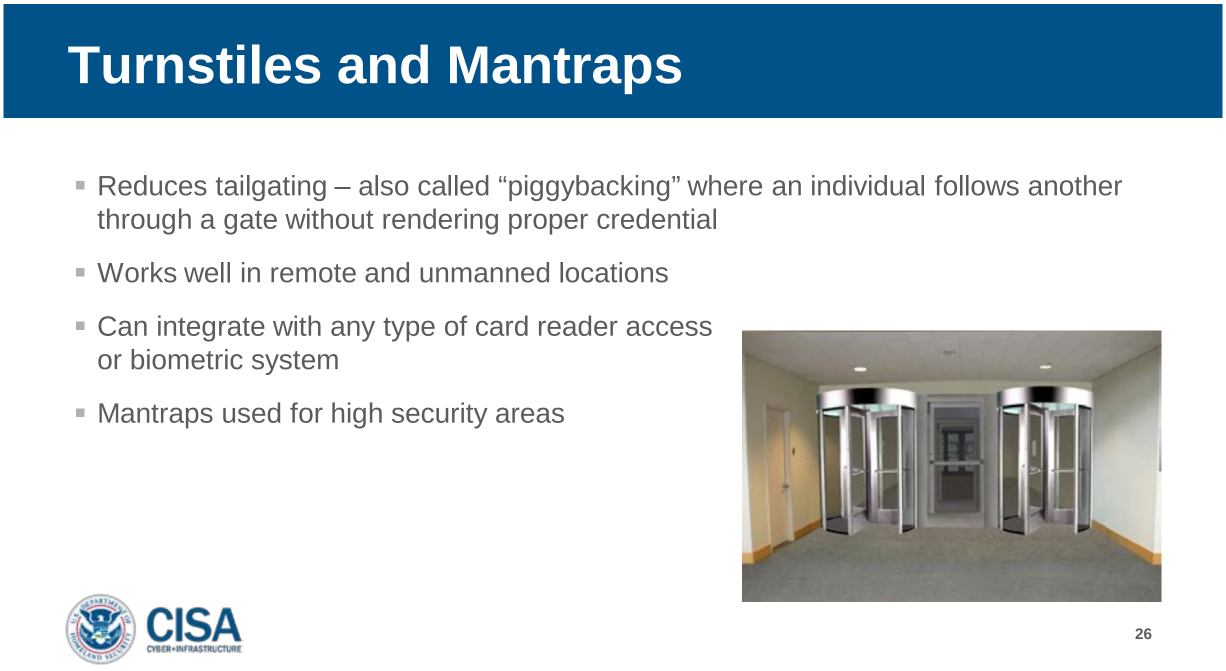
CYBER+INFRASTRUCTURE

25

**025 Then there's the classic lock, physical locks, and there's all different types-- rim locks, mortis locks, cylinder locks, cypher locks. Regardless of what you pick here, you really want to think about who is going to actually be retaining keys to these locks, what are they going to be doing with them, what are you trying to achieve.

Now, there's all different types like I said, and some of these may be susceptible to lock-picking more than others. Cypher locks, for example, are not as susceptible to lock-picking, but the problem there is they have different key combinations. People like to write key combinations down because they forget them often. So you got to be mindful of this because the cypher lock is only as good as how people are memorizing the numbers.

Turnstiles and Mantraps



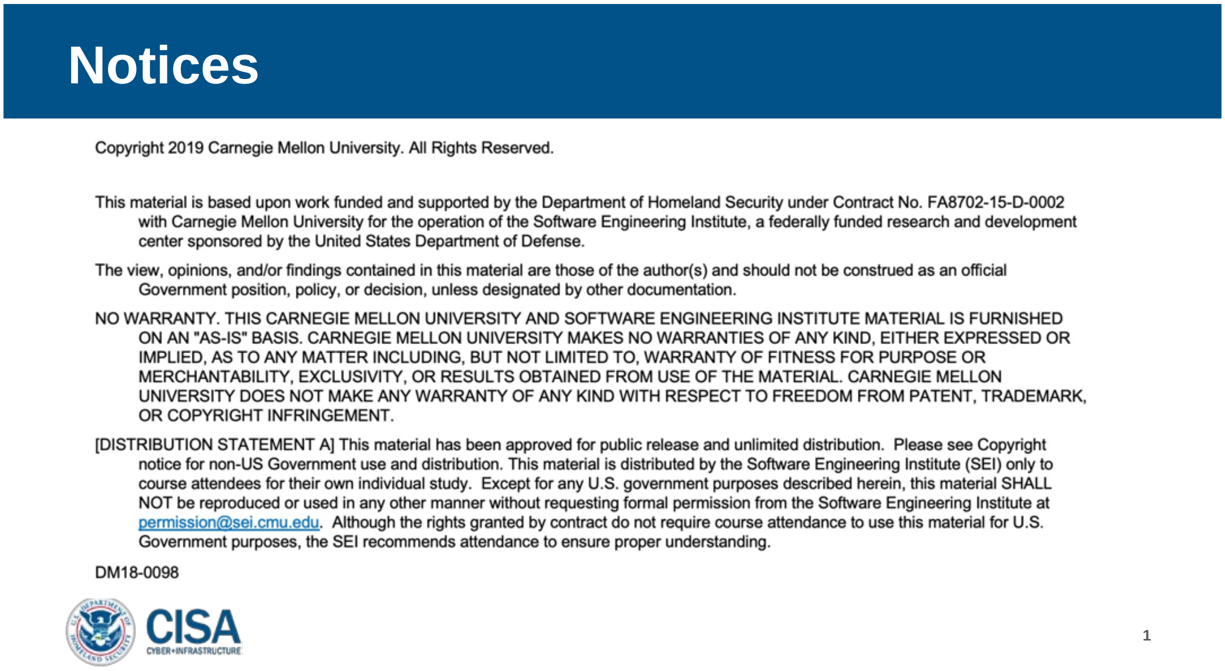
Turnstiles and Mantraps

- Reduces tailgating – also called “piggybacking” where an individual follows another through a gate without rendering proper credential
- Works well in remote and unmanned locations
- Can integrate with any type of card reader access or biometric system
- Mantraps used for high security areas

CISA
CYBER+INFRASTRUCTURE

**026 You can also have gates protected with turnstiles and mantraps. Now, there's a problem with this too. Usually you're going to want to monitor them some way because it's classic to have somebody tailgate or piggyback on somebody who's going in. So somebody who is properly credentialed will walk into the mantrap, and maybe someone follows directly right in behind him. This is really a classic too with locked doors. If I swipe a badge on a door and I actually swing the door open, walk through it, and forget that I had left it and it's swinging and someone maybe puts their arm in the door or something like that to hold it, and then they get in. You got to train your workforce so that they understand that that is not acceptable.

Notices



Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM18-0098